2020
NetSec-KR

스마트시티 보안 기술

– 블록체인 관점에서의 스마트시티 보안 –

부산대학교

김호원

부산대 컴퓨터공학과 교수
부산대 사물인터넷 연구센터장
부산대 블록체인 플랫폼 연구센터장

2020.7.16

목차

스마트시티 보안 - 블록체인 관점에서의 스마트시티 보안

I. 스마트시티 개요

II. 스마트시티와 블록체인

III. 블록체인 기반 스마트시티 UseCase

IV. 블록체인 주요 암호 기술

I. 스마트시티 개요

1. 스마트시티 개요
2. 미래형 스마트시티
3. 스마트시티 플랫폼

스마트시티 - 개요

스마트시티 개념 및 동향 (1/2)

- 세계 여러 국가에서 추진중인 스마트시티는 에너지/수자원 관리, 교통 문제 해결, 재난 대응 등, 도시 인프라의 효율적 관리에 집중
- 또한, 스마트시티는 시민이 직접 참여하며 데이터 기반으로 실질적 도시 문제 해결을 통해, 시민 삶의 질 향상 추구
  - 즉, 기술 적용/실증 차원이 아닌, 현실의 문제를 해결하는 것이 목표임
- 도시 전체가 하나의 통합된 체제로 운영되는 UOS(Urban Operating System) 추구
  - 이를 위해, 데이터 수집/가공/분석/활용을 데이터 플랫폼 및 데이터 거버넌스 체계 구축 필요, 보안 및 프라이버시 보호 필요

참고: 세계선도형 스마트시티 연구개발 사업, 수정기획보고서, 국토교통부, KAIA 2017

스마트시티 - 개요

스마트시티 개념 및 동향 (2/2)

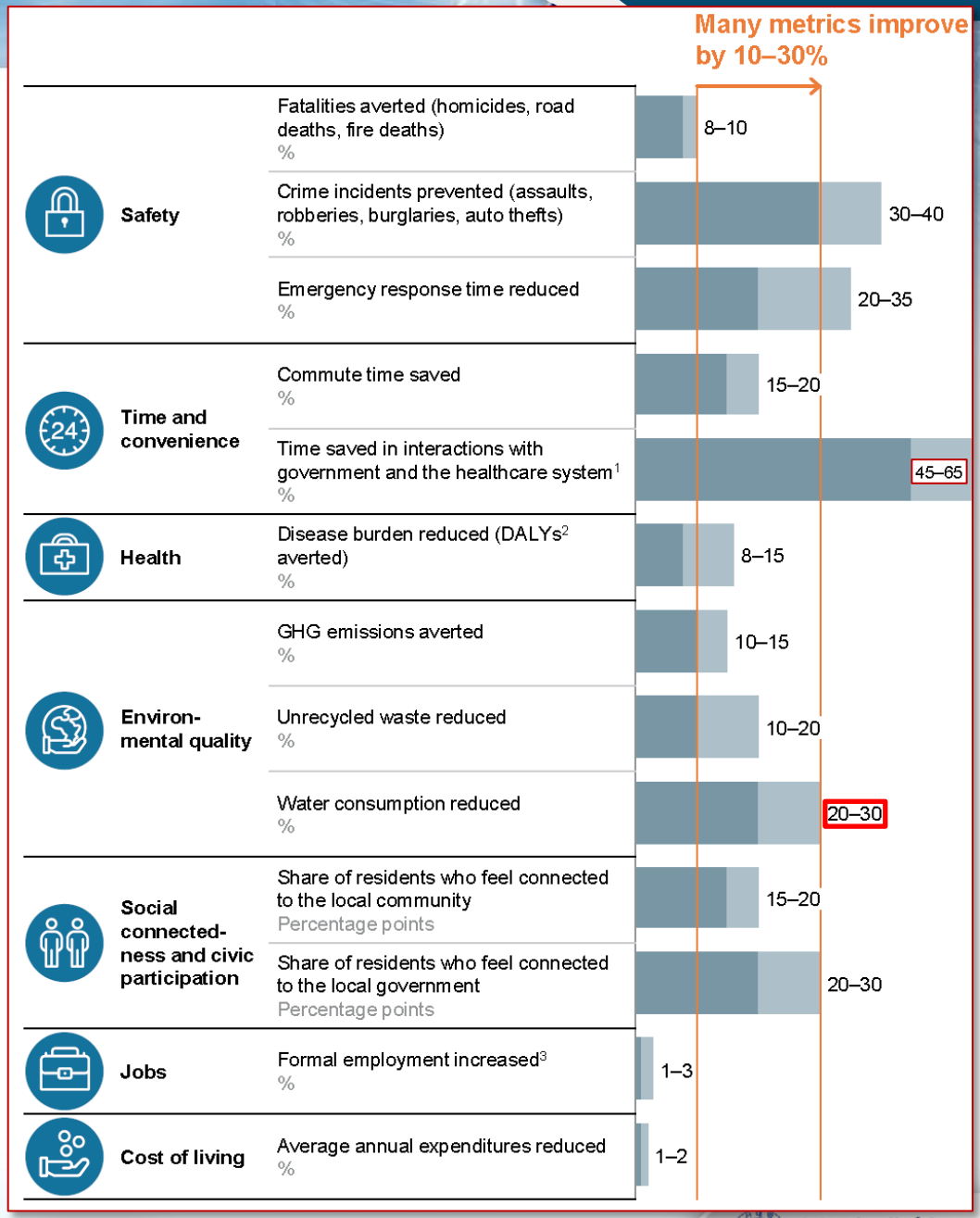
- 스마트시티는 ICT 기술 공급자와 시민 사용자간 조화 중요함
- 기존 공급자 위주로 진행 된 U-City 사업과 IoT 실증 사업 지양, 미래 스마트시티는 지속 가능한 스마트시티 서비스 생태계를 조성이 목표임
  - 시민의 삶의 질 향상에 도움되는 데이터 수집 및 가공/분석/활용
  - 공급자 위주의 스마트시티 솔루션 제공이 아니라, 시민과 지자체 니즈에 맞는 스마트시티 서비스 창출 필요

참고: 세계선도형 스마트시티 연구개발 사업, 수정기획보고서, 국토교통부, KAIA 2017

스마트시티 - 개요

스마트시티란?

- 스마트시티는 시민의 삶의 질을 향상시키고 지속가능하도록 만듦
- 주요 생활 지표를 향상시킴
- 현재 수준의 스마트시티 실현 기술 적용할 경우의 주요 특성
- 안전, 편의성, 건강/복지, 환경 분야 향상 효과 큼
- 일자리 및 생활비 절약 효과는 상대적으로 낮음



참고: McKinsey Global Institute Analysis Report

스마트시티 실현 기술 1- IoT, 블록체인, AI

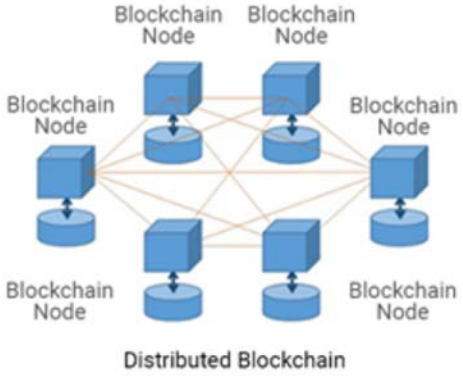
데이터 수집/생산 (IoT), 데이터 신뢰성(블록체인), 데이터기반 고부가치 창출(AI)

- 사물인터넷은 유무형의 사물을 데이터/서비스와 연결하며,
- 블록체인은 해당 데이터의 신뢰성을 높이고,
- AI는 해당 데이터로부터 의미있는 정보와 지식을 추출함 → 이에, 기존 산업/분야의 경쟁력/효율성을 높이며, 신규 산업 창출도 가능함

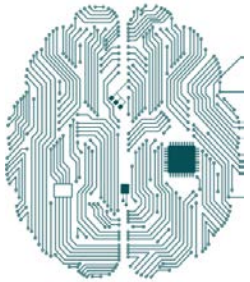
- IoT에 AI, 블록체인 융합시, 관련 시장 획기적 성장 (Forbes 2018.1, IBM)
  - IoT, AI의 높은 산업 확장성과 블록체인의 고신뢰, 투명성 결합시 높은 시너지 효과 발휘
  - 2022년 IoT(스마트가전)와 블록체인 융합시 세계 총 시장 규모는 296조 예상

디지털 변혁을 위한 Trinity 기술

IoT 기술
(1차/2차/3차산업 전산업 적용 등)



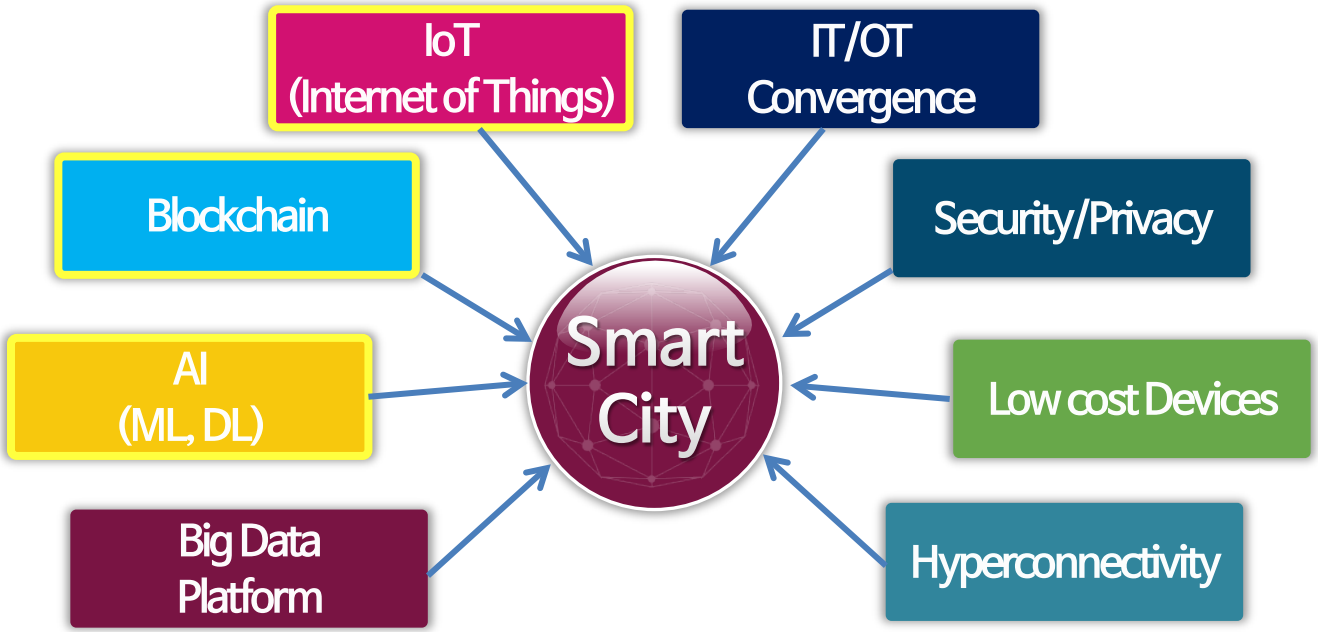
블록체인
(고신뢰/투명성, 분산원장, 스마트 컨트랙트, 분산DB)



인공지능 기술
(데이터분석, 머신러닝, 딥러닝, 추론 등)

스마트시티 실현 기술 2

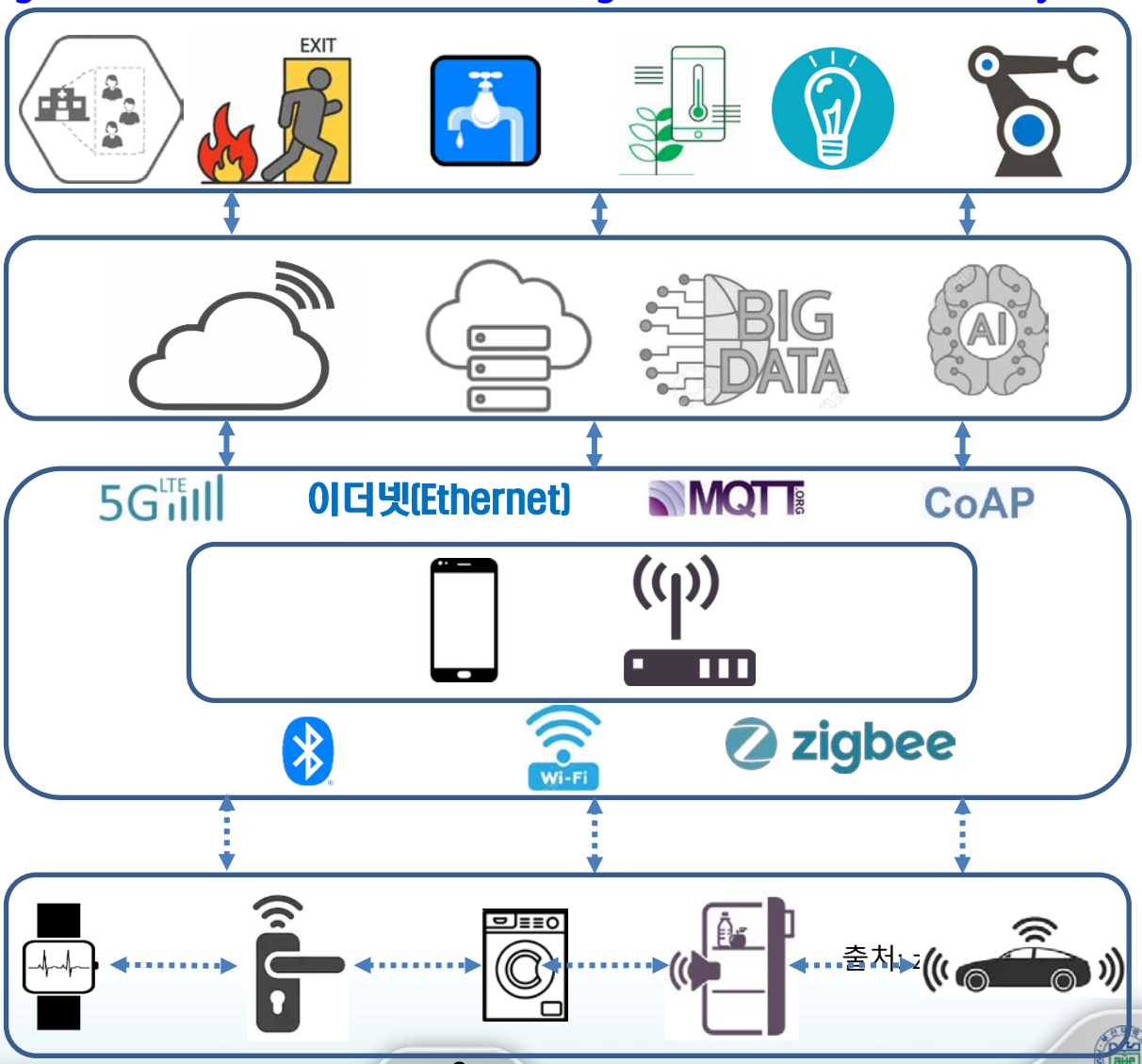
- 스마트시티 실현을 위해선 다양한 IoT, OT 기술 필요
  - IoT, Blockchain, AI 외에, IT/OT 융합, 디바이스, 초연결성, 보안 및 프라이버시 등



출처: zdnet

스마트시티 구현 주요 기술 - IT 기술 중심

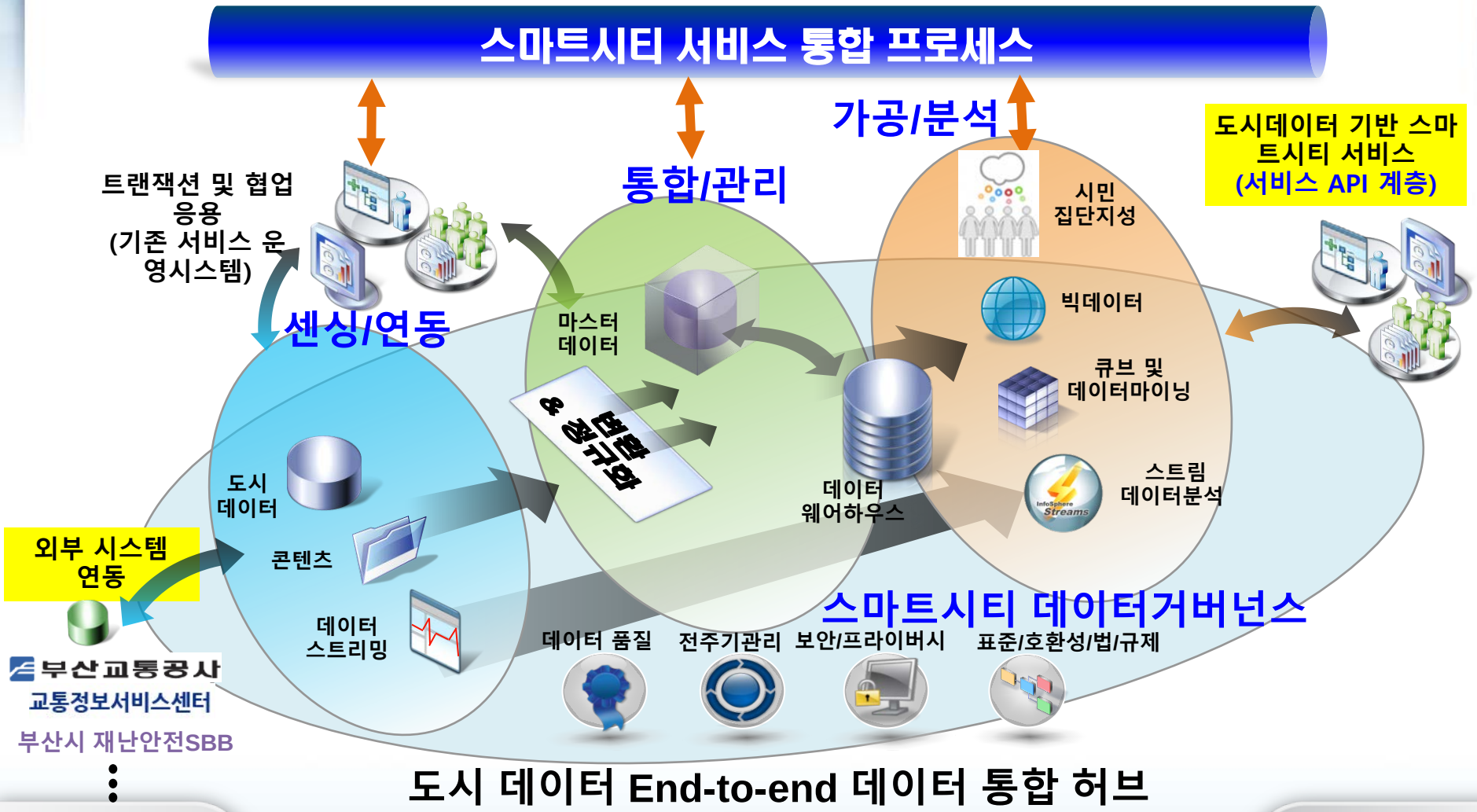
- **IoT is the infrastructure for Smart City**
  - Understanding IoT structure → Understanding data flow in Smart City



스마트시티 = 데이터시티

사물인터넷 기반 스마트시티 실현

- 지능형 데이터 허브에 기반을 두는 데이터 기반 스마트시티

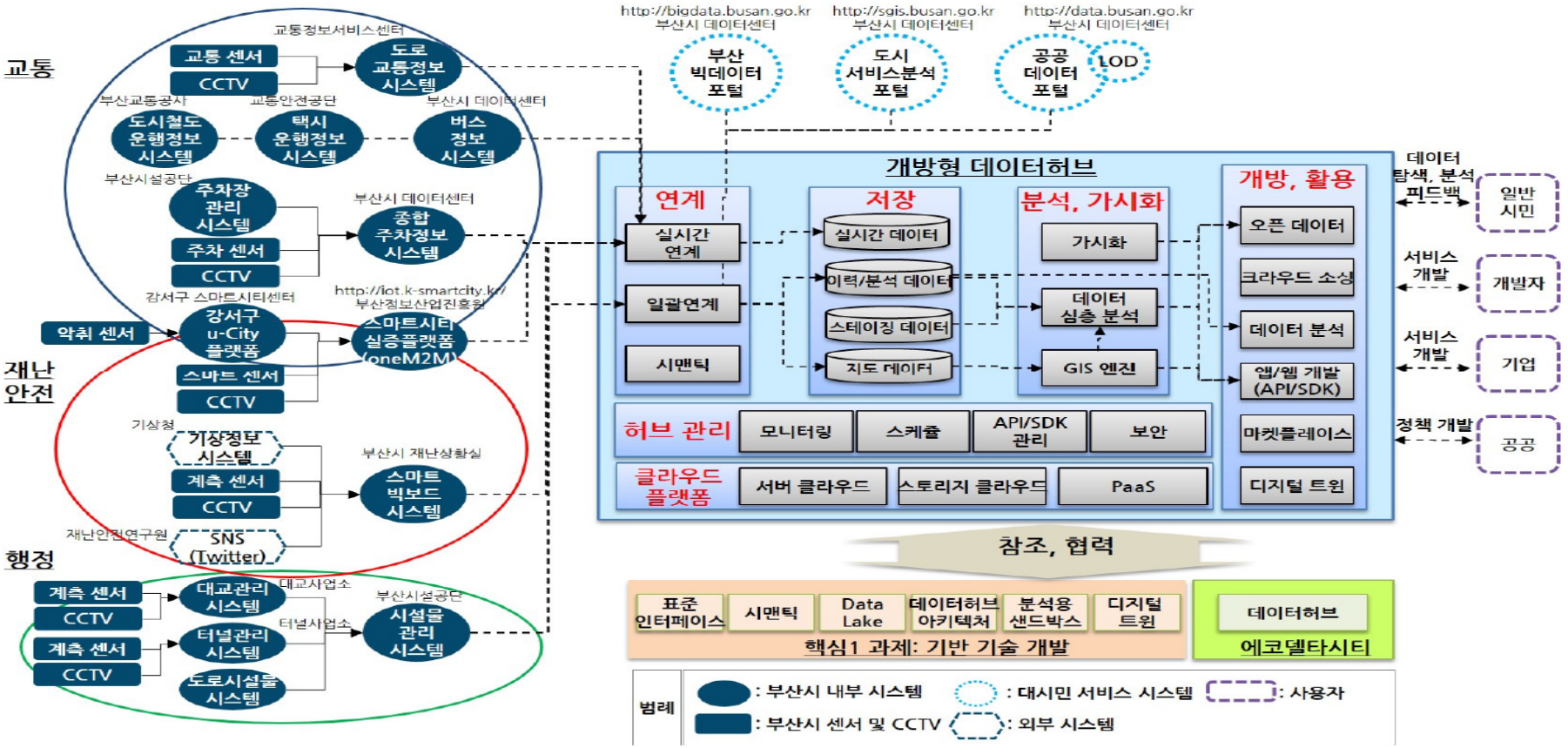


데이터 기반 스마트시티 1 - 부산 스마트시티

데이터 기반 스마트시티 실현을 위한 데이터 허브

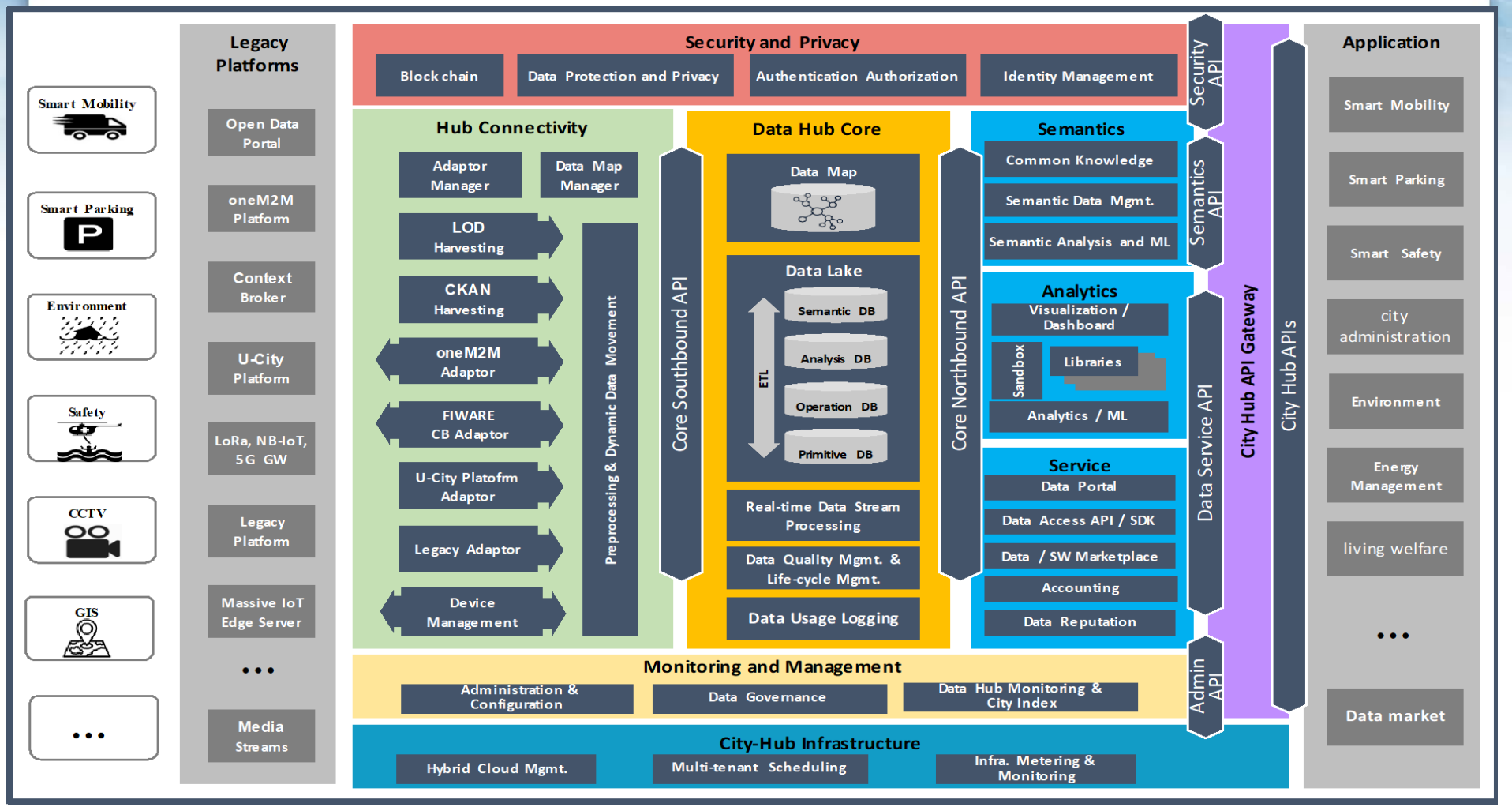
▪ 부산 스마트시티 서비스(교통, 안전, 시설물 관리, 행정)와 데이터 허브

- (교통 분야) 부산 교통정보시스템, 교통공사 도시철도시스템, 부산시 버스정보시스템, 종합주차정보시스템 연계
- (안전 분야) 부산시 스마트빅보드시스템(재난 관제), 과기정통부 스마트시티실증플랫폼(oneM2M) 연계
- (시설물 관리 및 행정 분야) 부산시설공단 시설물관리시스템 DB연계(광안대교, 터널, 도로시설물 정보) 등



데이터 기반 스마트시티 2 - 국토부 사업, KETI

Use case & requirement | City Hub Architecture | Standard & Global Collaboration | Data Model & Ontology | Integration | Verification & Validation



Law and System | Data Catalog | Data Governance Committee | City Hub Alliance | Grant Program | Project Management

참고: KETI City Hub 자료

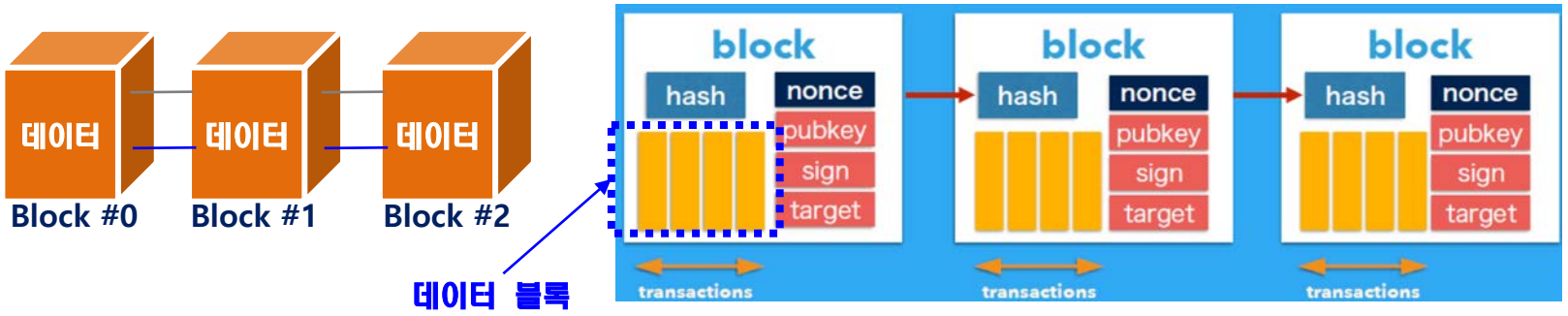
Ⅱ. 스마트시티와 블록체인

1. 블록체인 개요
2. 블록체인 관련 주요 용어
3. 블록체인 주요 장점
4. 블록체인 기반 서비스

블록체인 개요

블록체인(Blockchain) 어원

- 블록(데이터, 거래원장)이 체인(chain)으로 계속 연결됨



블록체인 정의

- 비즈니스 네트워크 참여자들의 자산(유/무형 자산)을 스마트 컨트랙트(Smart Contract) 기반으로 거래를 투명하게 공유하는 기술 (IBM)

- 블록(소규모 데이터)을 P2P 방식으로 생성된 체인형태의 분산 데이터 저장 환경에 저장함. 저장된 블록은 임의 수정 및 변경이 불가능한 데이터 위변조 방지 기술 (wikipedia)

- 거래정보를 기록한 원장(ledger)을 (특정 기관의 중앙 서버가 아닌) P2P 네트워크에 분산하여 참가자가 공동으로 기록하고 관리하는 기술 (한국은행) → Public 블록체인

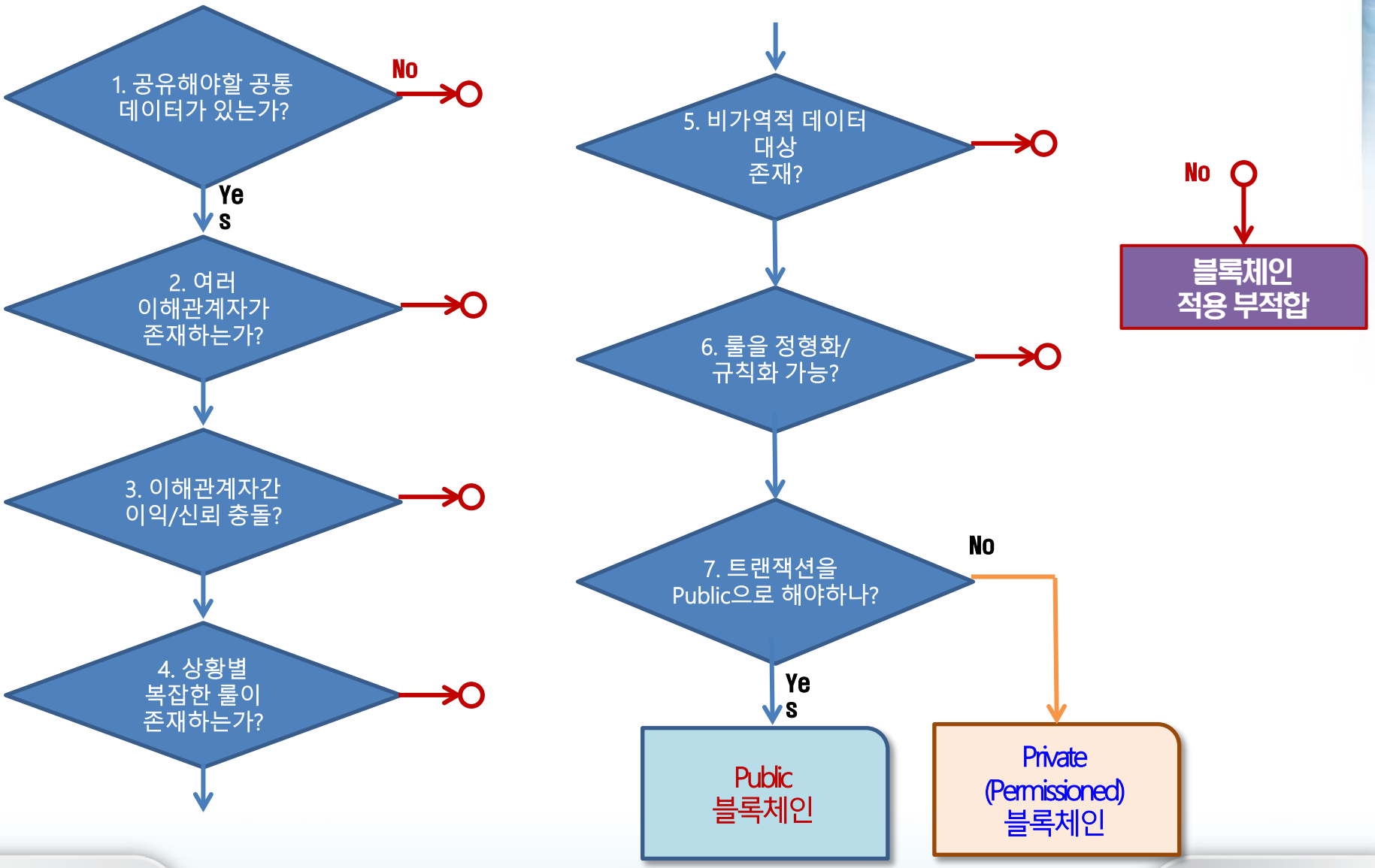
블록체인 기반 서비스 - 적용시 장점

산업별 블록체인 도입 분야 및 도입시 장점

금융	•해외 지불 결제, 무역 거래, 규제 및 감리, 돈세탁 방지, 고객 인증, 보험, P2P 거래 •기존 비효율적 금융 처리 흐름 개선 및 처리 시간 단축, 저비용 실현 등
제조, 물류유통	•SCM, 콜드체인, 경매 서비스, 식품 유통 추적 등 •개선된 물류 공급망 관리 및 투명성/신뢰성 향상, 추적성 향상
헬스케어	•환자와 의사(병원), 외부 기관, 보험 회사와의 직접적 정보 교환 가능 • 제 3의 인증 기관 불필요
행정, 공공서비스	•기록물 관리, 전자 투표, 세금, 공공 부동산 관리, 금융 감독, 법률 관리 등 • 규제 집행의 투명성 향상, 사기 감소, 행정 효율성 향상 등
사회/문화 경제	•음원, 디지털 콘텐츠 관리, 티켓 서비스, 사치품 거래, 미술품 거래, 저작권 보호 •자동차 리스, 재화 공유, 숙박, 공유 경제, 부동산 거래 등
미래 산업	•사물인터넷, 자율주행 자동차, 스마트그리드 실현 •신뢰성, 자동화 등으로 인한 신산업 창출

블록체인에 적합한 서비스

블록체인 적용 대상 서비스 분야 선정시 고려할 점



블록체인의 진화

코인에서 서비스 산업으로 진화하는 블록체인

- 분산원장에 대한 개념 증명
- 2009년 Satoshi Nakamoto 비트코인 소개 → 익명 합의에의한 분산원장 개념
- 비트코인, 라이트코인 등

- 화폐 유통, 디지털 지불 등 암호 화폐 개념 정립
- 거래 중심의 블록체인 개념 정립

- 화폐 유통 수준을 넘어서서 금융 시장 및 타 응용 분야로 확대
- 스마트 컨트랙트 중심의 블록체인 개념 정립

- 헬스케어, 행정 서비스, 콘텐츠, 문화 등 다양한 분야로 확대
- 서비스 플랫폼 개념 정립
- 이더리움, 하이퍼레저, 스팀 등

Ⅲ. 블록체인 기반 스마트시티 UseCase

1. 데이터 마켓 플레이스

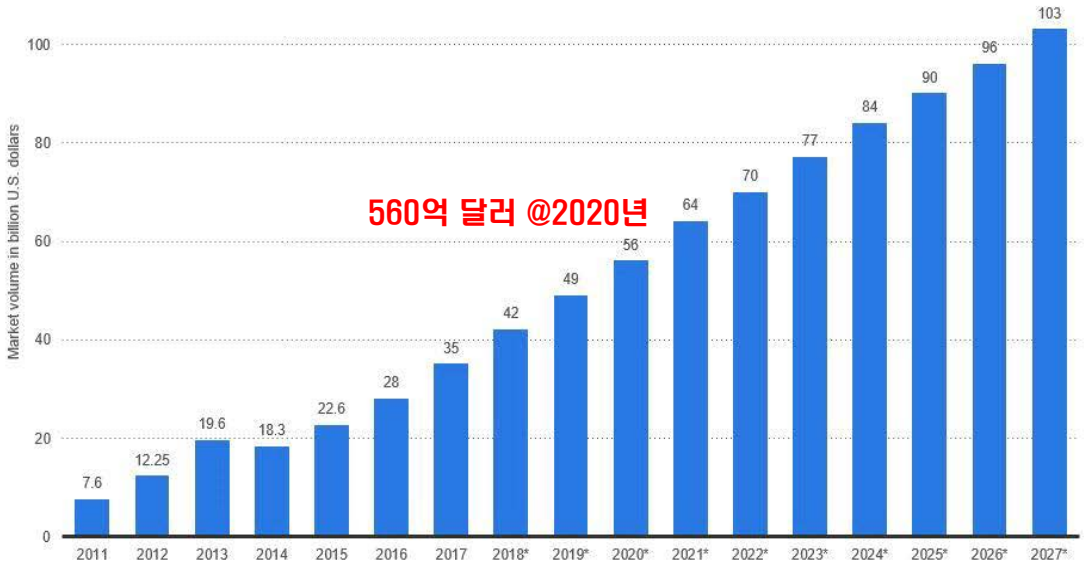
블록체인 기반 데이터 마켓 플레이스

데이터 마켓 플레이스 개념

- 스마트시티 등, 공공/민간에서 대규모 데이터 수집 및 관리, 거래 수요 발생
- 이에, 데이터 마켓 플레이스가 필요하며, 이를 통한 데이터 경제 활성화 예상

Forecast Revenue Big Data Market Worldwide 2011-2027

Big Data Market Size Revenue Forecast Worldwide From 2011 To 2027
(in billion U.S. dollars)



[빅데이터 마켓 성장 추지 전망(2011~2027 - Wikibon and reported by Statist]

블록체인 기반 데이터 마켓 플레이스

국내외 공공 데이터 포털 현황

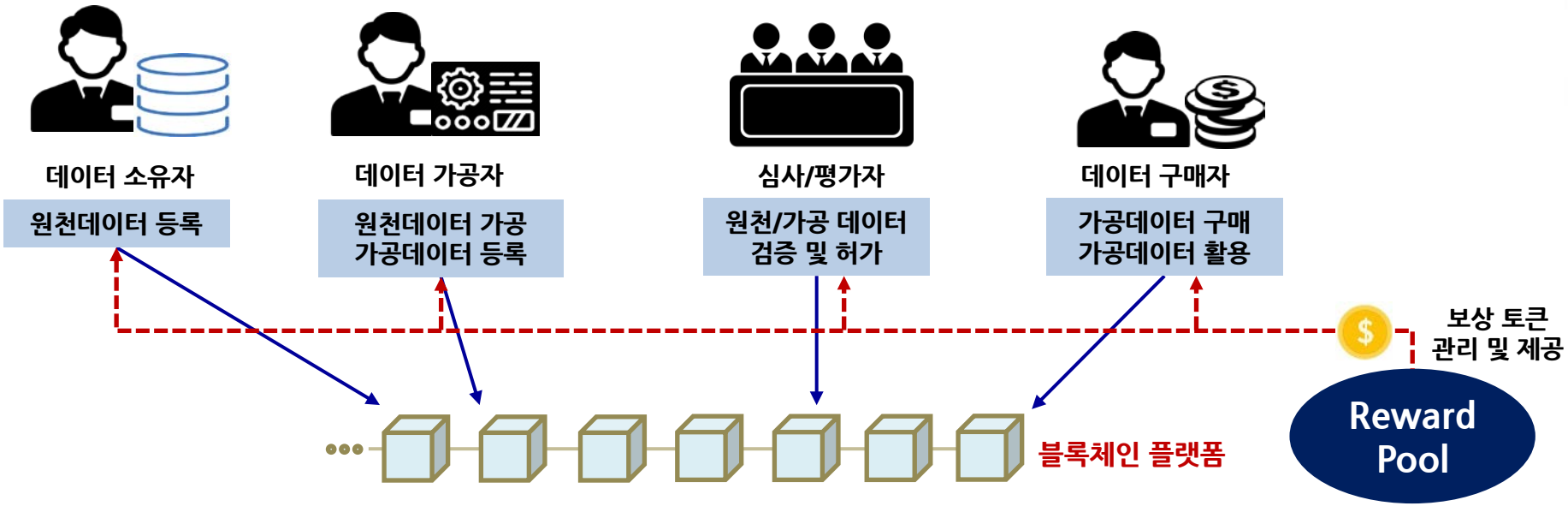
*주요국의 공공데이터 플랫폼 운영 현황('18. 7. 17. 기준 - 정보통신기술진흥센터)

국가	주소	데이터셋	특징
영국	data.gov.uk	• 경제, 환경, 지도, 범죄·법, 국방, 정부지출, 교육, 건강, 교통 등 12개 분야 44,086개의 데이터셋	• CKAN(Comprehensive Knowledge Archive Network)을 활용하여 '10년 공공데이터 포털 구축 • 국무조정실 산하 정부디지털서비스청(Government Digital Service)에서 운영
캐나다	open.canada.ca	• 농업, 경제·산업, 교육·훈련, 정치, 건강·안전, 정보통신, 노동, 법, 군사, 과학기술, 사회문화, 교통 등 19개 분야 80,914개의 데이터셋	• 개발자를 위한 도구인 'Code for Canada'를 제공, 혁신적이고 창의적인 응용 프로그램 개발 지원
프랑스	data.gouv.fr	• 농업, 문화, 경제, 교육 및 연구, 지속가능한 에너지, 건강, 사회, 교통 등 9개분야 33,157개의 데이터셋	• 다양한 이해관계자들이 공동으로 시스템을 구축하는 오픈소스 방식으로 운영 • 팔로잉, 업데이트 및 제거 정보, 댓글 실시간 확인, 알림 기능, 자료 전송 기능 탑재 등 실시간 이용자 활동 공개
미국	data.gov	• 농업, 기후, 교육, 에너지, 금융, 건강, 지방정부, 과학연구 등 14개 분야 285,810개의 데이터셋	• CKAN(데이터)과 Wordpress(컨텐츠)를 통합하여 포털 운영 • GitHub에 소스 코드를 공개하여 자유로운 데이터 편집·추가 기능
일본	data.go.jp	• 재무행정, 경제, 사법, 안전, 교통, 인구, 정보통신, 과학기술 등 17개 분야 21,647개의 데이터셋	• 메타데이터를 종류별로 일괄 다운로드할 수 있도록 제공 * JSON, CSV 포맷으로 제공
한국	data.go.kr	• 교육, 국토관리, 공공행정, 재정금융, 산업고용, 사회복지 등 16개 분야 24,990개의 데이터셋	• 오픈API(2,521개)와 LOD 서비스를 제공하여 데이터 활용도 제고 노력 • 사용자 수요가 높은 분야를 선정하여 활용이 용이한 형태로 가공된 대용량의 국가중점데이터 제공

블록체인 기반 데이터 마켓 플레이스

블록체인 기반 데이터 마켓 플레이스

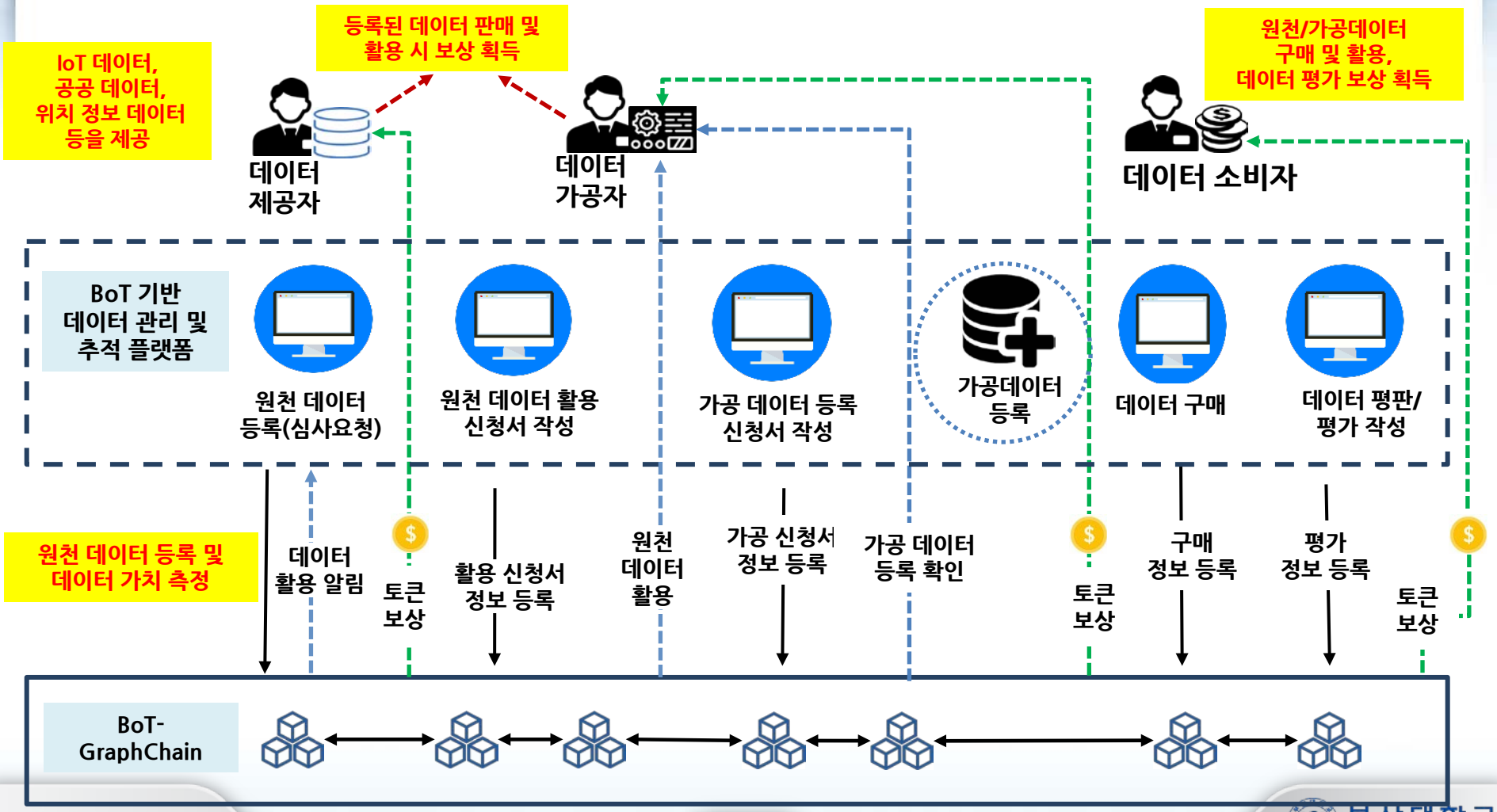
- 기존 데이터 마켓은 데이터 품질 문제 있음 - 무결성 및 신뢰성, 투명성 문제
- 또한, 마켓 플레이스 사용자 많지 않음 → 데이터 생태계 조성 실패
- 블록체인을 통한 데이터 품질 향상, 신뢰향상, 거래 활성화
  - 예: 스마트컨트랙트 기반 데이터 관리(등록, 평가, 구매 등), 참여자 보상 제공



블록체인 기반 데이터 마켓 플레이스

블록체인 기반 데이터 마켓 플레이스

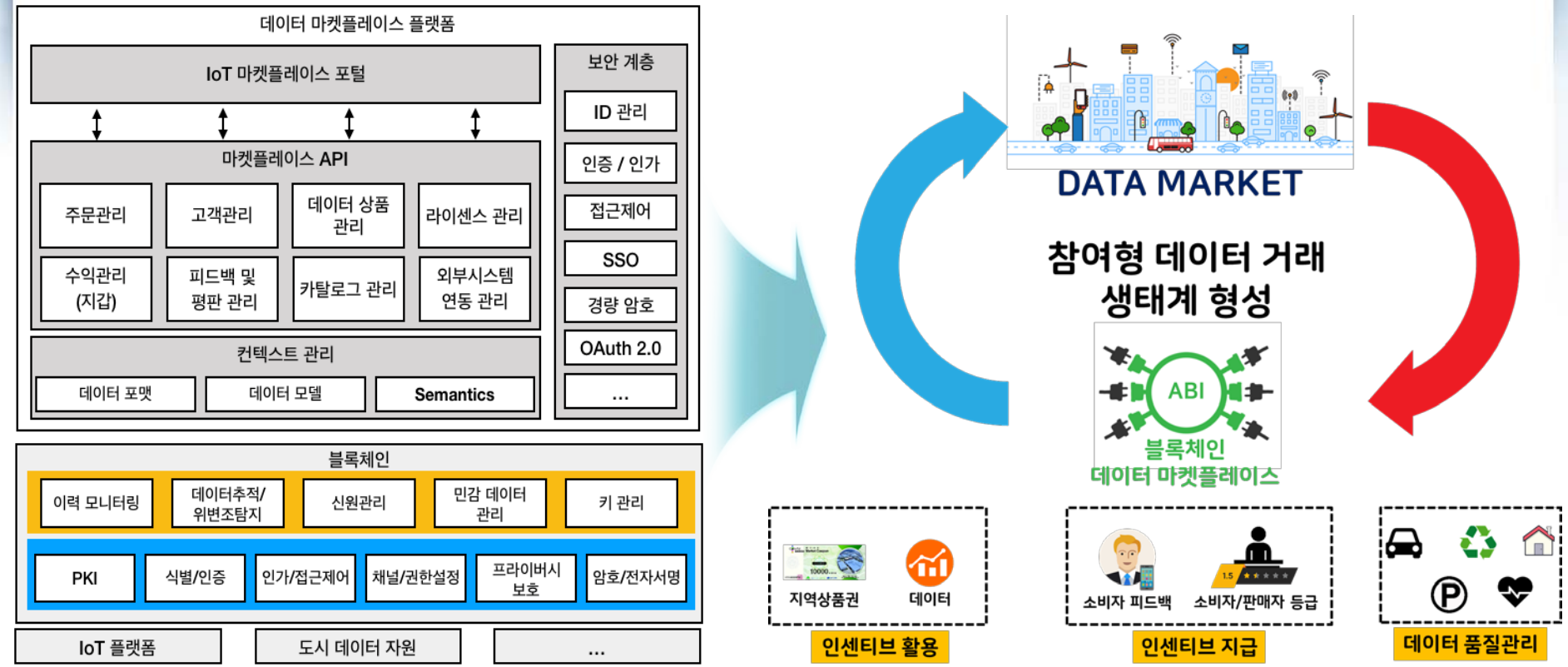
- 데이터에 대한 무결성 및 투명성 보장, 토큰 보상 기반 데이터 제공자, 사용자 확대
- 데이터 생성에서 거래, 가공, 활용, 품질 평가 등 기능 제공



블록체인 기반 데이터 마켓 플레이스

블록체인 기반 데이터 마켓 플레이스 사례

- 블록체인과 보안, 마켓 플레이스 API, 서비스 플랫폼 제공을 통한 데이터 생태계 제공



[블록체인 기반 데이터 마켓 플레이스 예시]

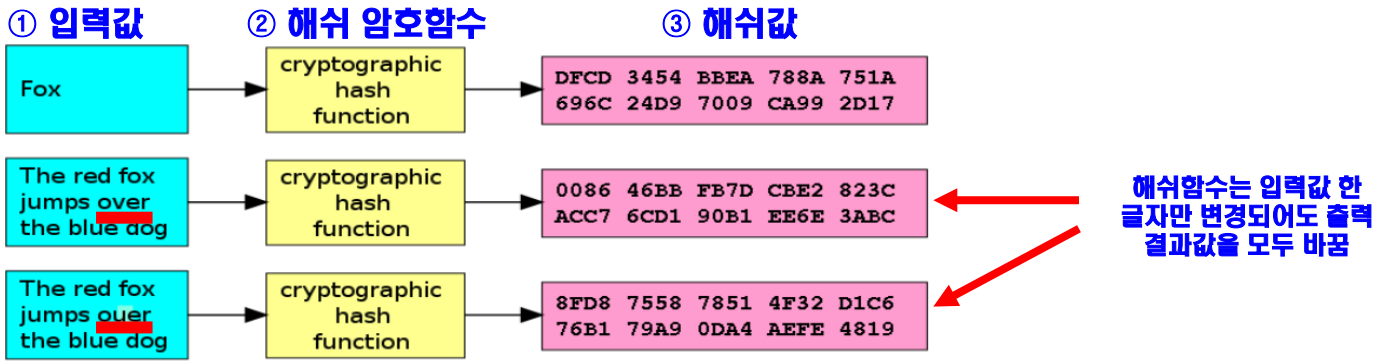
Ⅳ. 블록체인 주요 암호 기술

1. 해쉬함수와 데이터신뢰성
2. 블록체인과 프라이버시 보호
3. 온체인과 오프체인 기법
4. 공개키 기반 식별(Identification)과 정보 유출
5. 익명 Credential 기법
6. 영지식 증명 기법

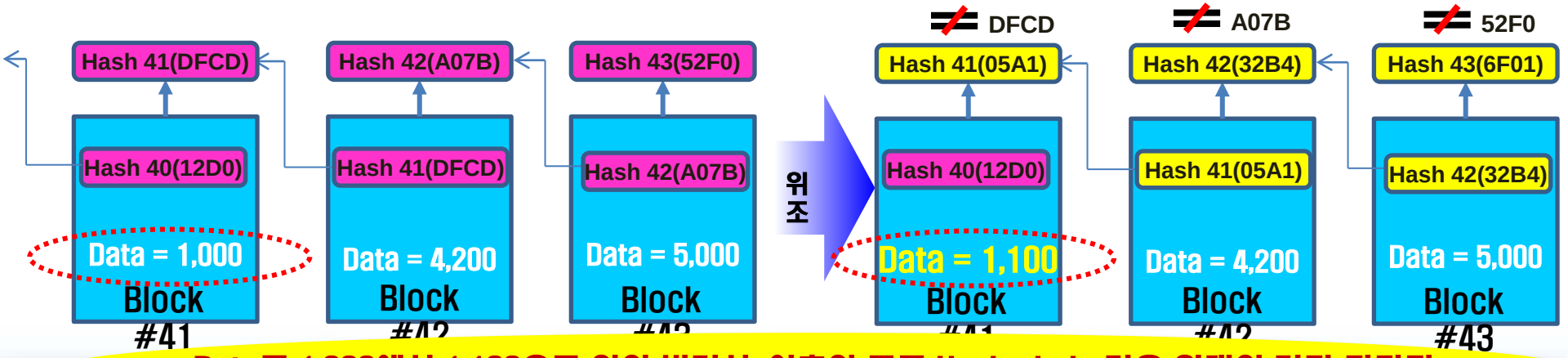
해쉬함수와 데이터 신뢰성

해쉬 함수(체인)

- 해쉬함수는 임의의 길이 데이터를 고정된 어떤 값(해쉬값)으로 만드는 암호 함수
  - 해쉬값(출력값)과 동일한 다른 입력값을 찾는 것은 매우 어려움



- 해쉬 체인에 있는 특정 블록 데이터 수정시, 이후 해쉬 체인 값이 모두 바뀜(불법적 위변조 탐지됨 → 변경 불가)

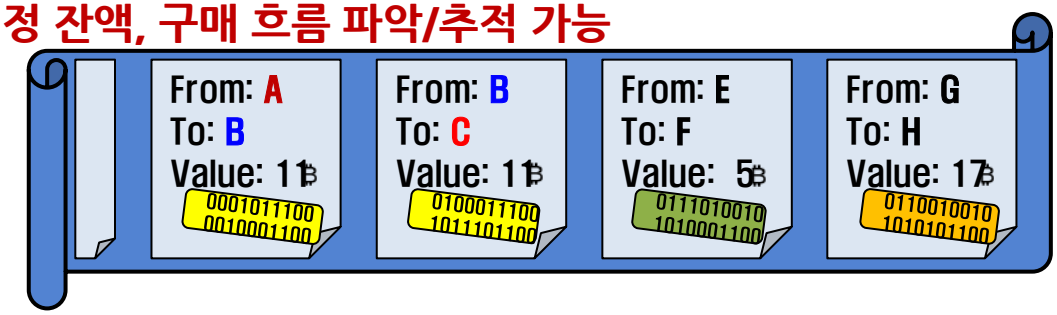


Data를 1,000에서 1,100으로 임의 변경시, 이후의 모든 Hash chain 값은 원래의 값과 달라짐

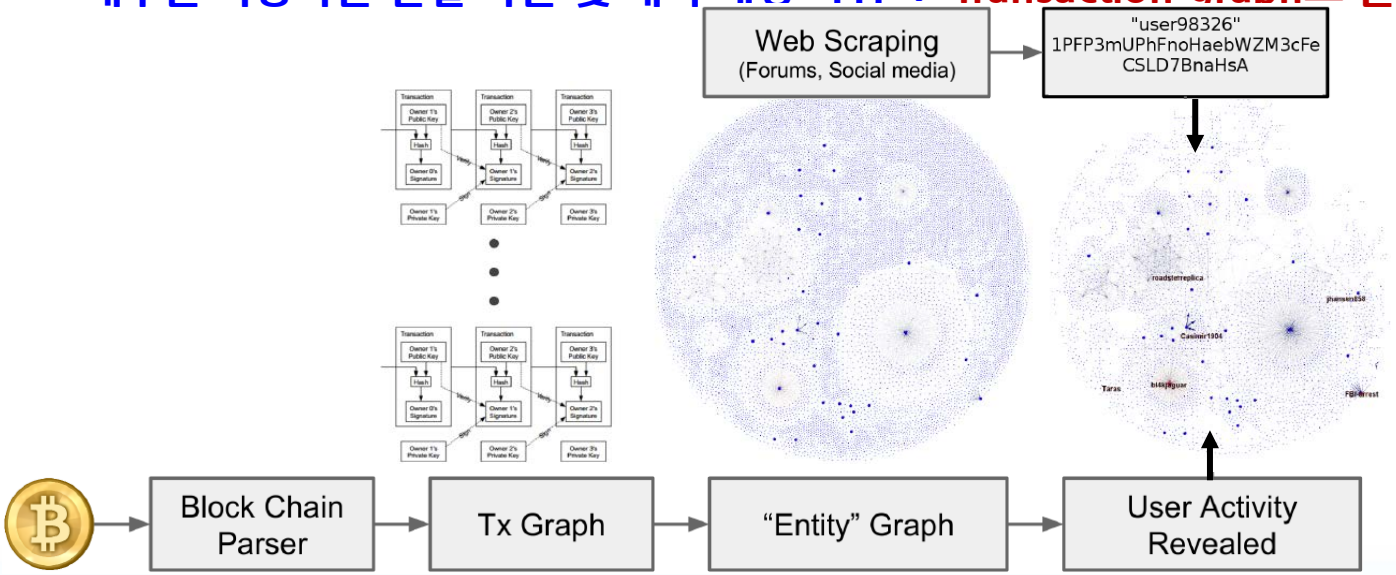
블록체인과 프라이버시 보호 - Public 블록체인

Bitcoin에서의 프라이버시 이슈(Public 블록체인)

- Bitcoin의 기본 구조(Public ledger에 모든 transaction broadcasting) → 프라이버시 침해
- 구매 여부, 계정 잔액, 구매 흐름 파악/추적 가능



- Pseudonym을 사용하지만,
  - 대부분 사용자는 단일 혹은 몇 개의 계정 가짐 → Transaction graph로 분석 가능



- 참고문헌 [1,7]

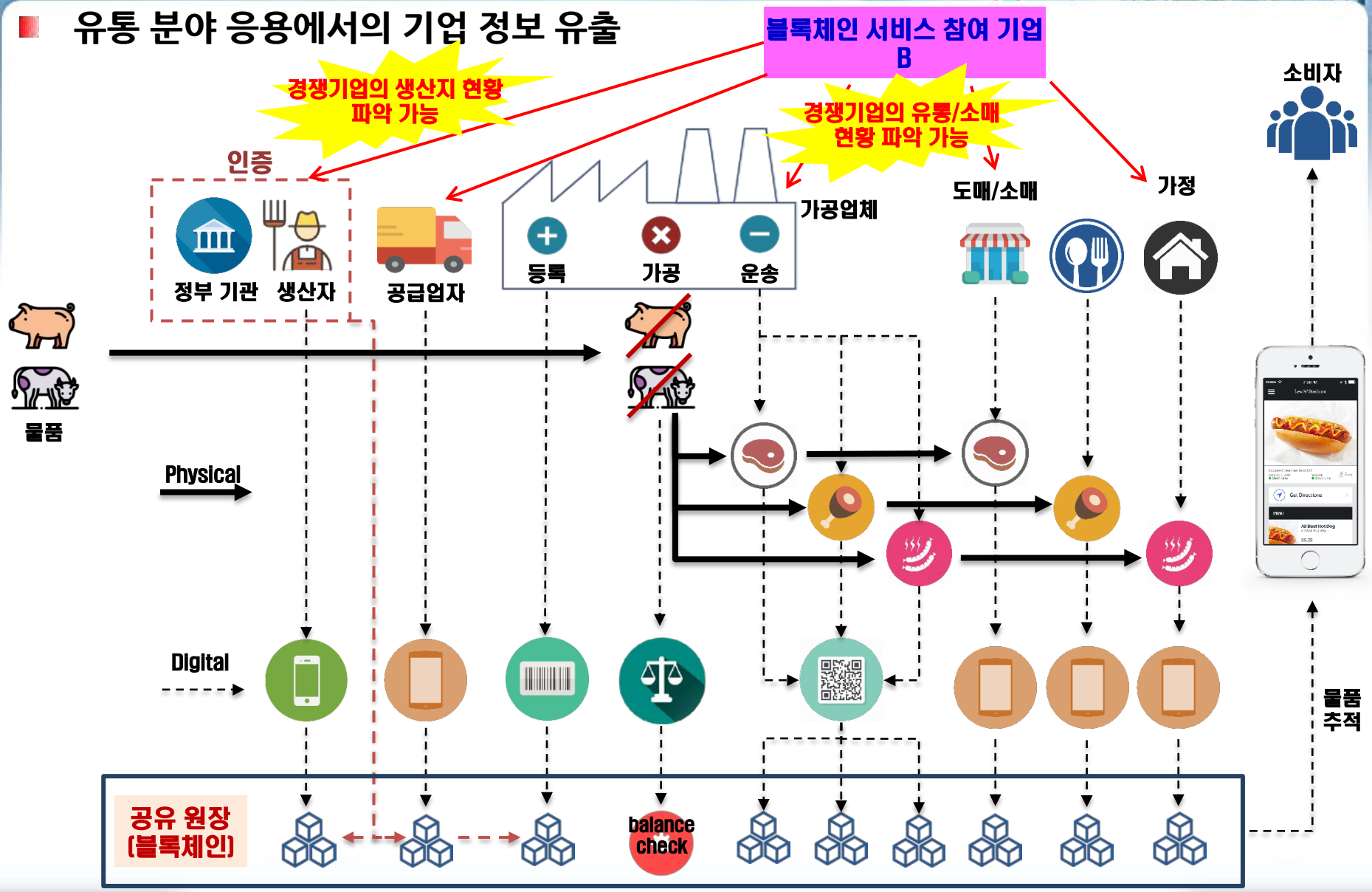
블록체인과 프라이버시 보호 - Private 블록체인

- Public뿐만 아니라, Private 블록체인상에서도 중요한 프라이버시 이슈
  - 전형적인 물류/유통 응용에서의 다수의 이해 관계자간 정보 공유를 통해, 정보 투명성/일관성/신뢰성 제공함
  - 이는 필연적으로 경쟁 기업에 의한 기업 프라이버시 침해 발생 - 블록체인 확산 저해 요인

〈 다수의 이해관계자들이 참여하는 육상/해상 물류 흐름도 〉

블록체인과 프라이버시 보호 - Private 블록체인

유통 분야 응용에서의 기업 정보 유출



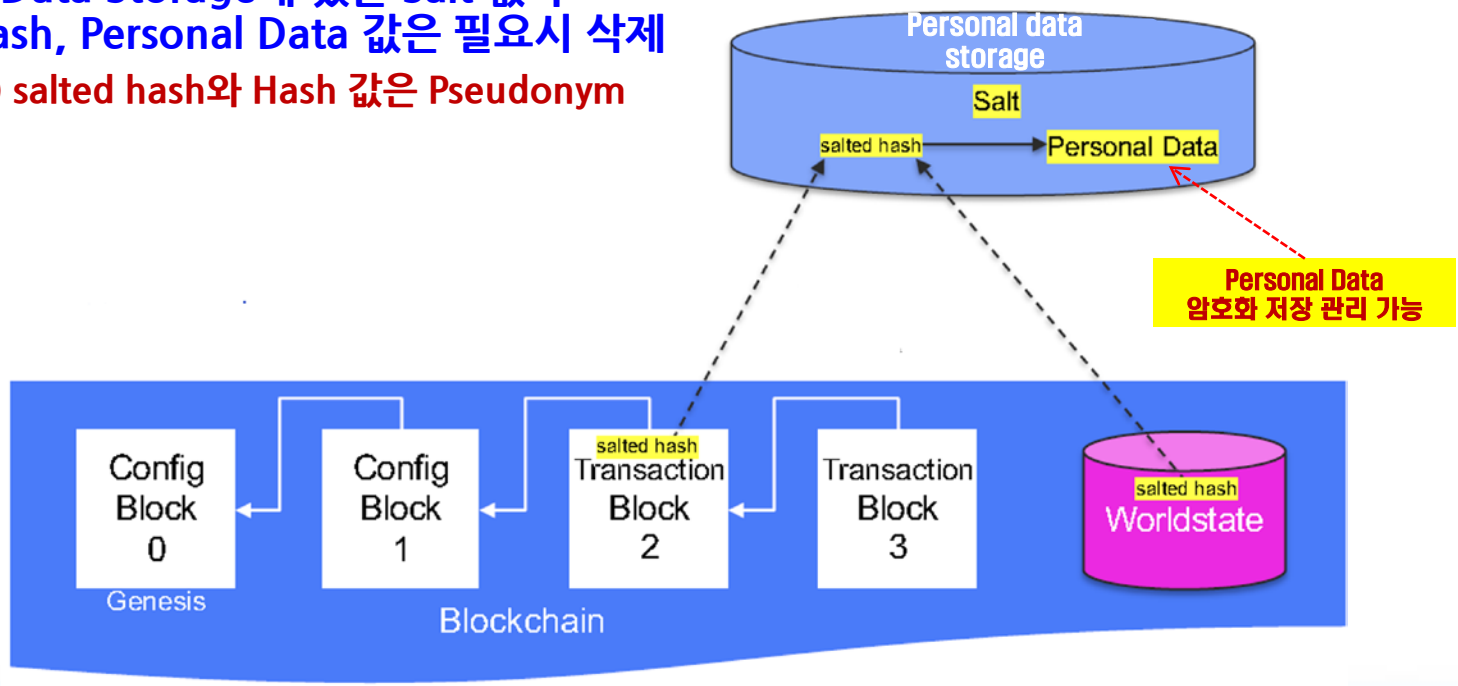
참고: Provenance사의 블록체인 사용 예

블록체인과 프라이버시 보호 - On-chain과 Off-chain

오픈체인 방식을 통한 프라이버시 보호 1

- 개인/기업의 데이터(Personal Data: PD)는 off-chain 데이터 스토리지에 저장 → 즉, Personal Data는 블록체인의 블록에 저장되지 않음
- On-chain(블록체인)에는 데이터에 대한 salted hash 값을 저장 → On-chain은 결국 "Distributed hash table"
  - Salted hash 값은 PD 데이터에 링크 제공
  - Salt 값은 각 프라이버시 데이터에 유일하며, 안전하게 저장

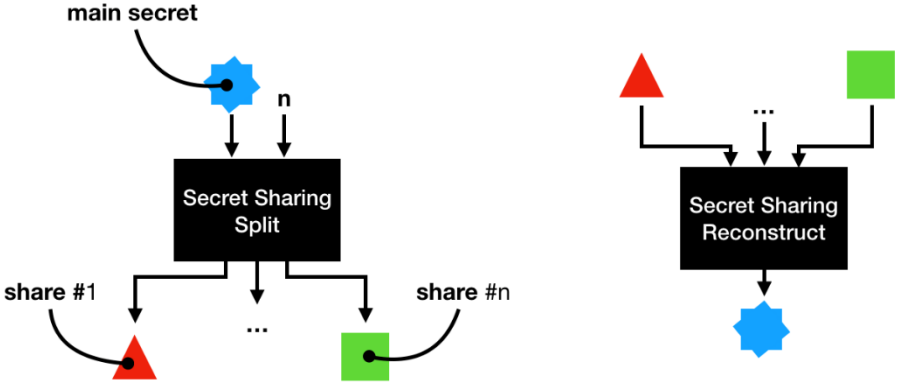
- Personal Data Storage에 있는 Salt 값과 Salted Hash, Personal Data 값은 필요시 삭제
  - 참고) salted hash와 Hash 값은 Pseudonym



블록체인과 프라이버시 보호 - On-chain과 Off-chain

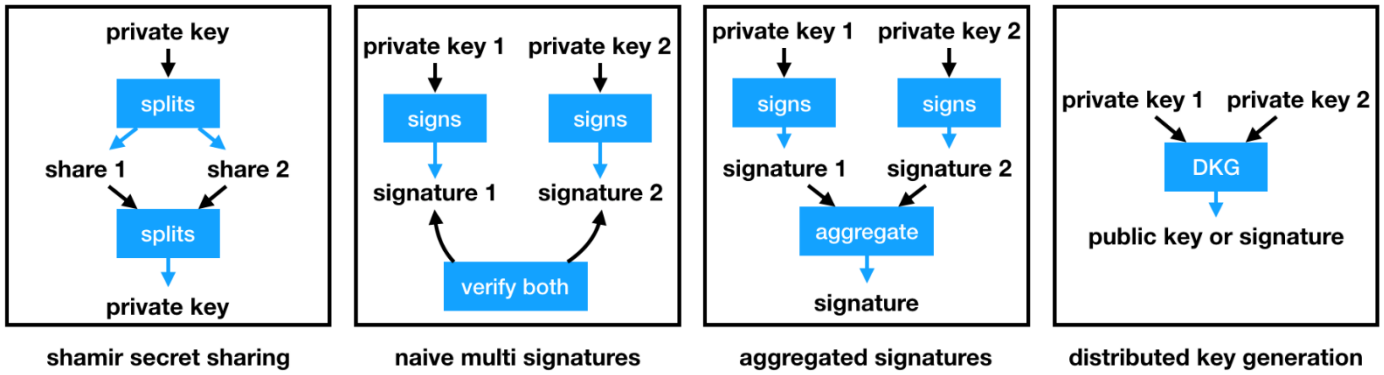
오픈체인 방식을 통한 프라이버시 보호 2

- Personal Data는 off-chain Personal Data Storage에 암호화되어 저장될 수 있음
- threshold encryption (Secret Sharing), Multisignature 등 사용



- 암호화 key 값을 분산 저장함
- 비밀정보를 n개로 분할 → 향후 k개만 있으면 복원 가능
- 단점: 복구를 위해 선택된 k개의 분산 저장된 키가 손상(single point of failure)되면, 키 복구 어려움

〈 Shamir Secret Sharing 기법: (k, n) 기법 개념도〉

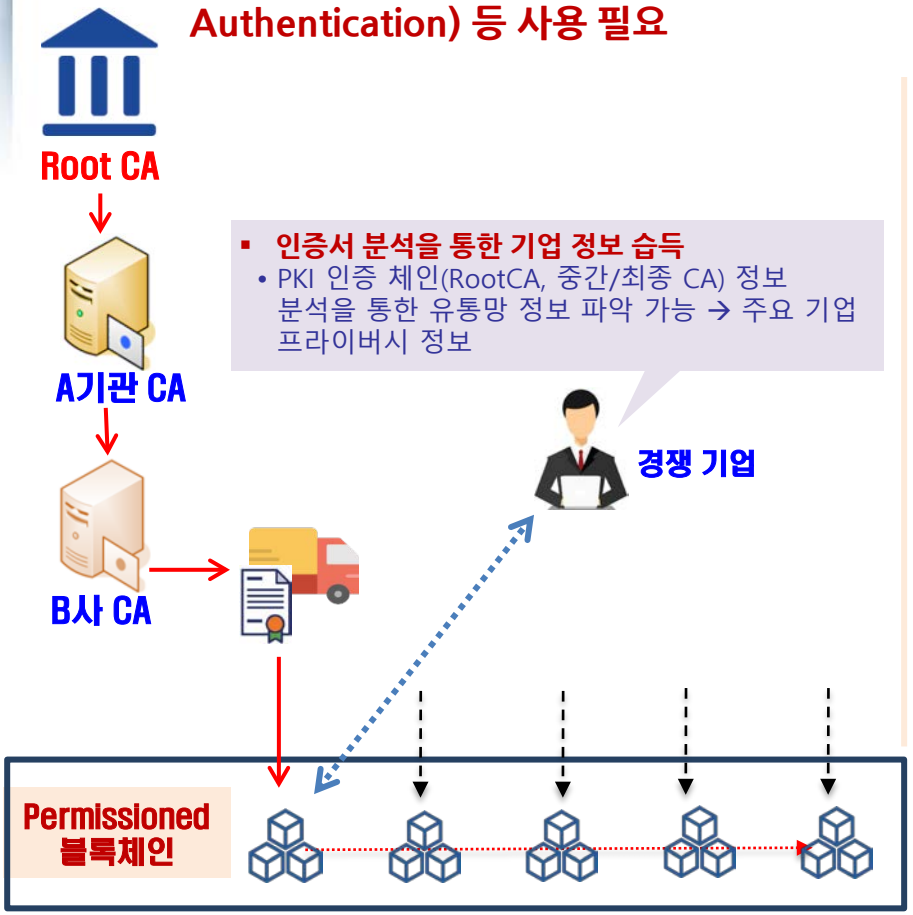


- multisignature 기법 혹은 aggregated signature 등도 사용 가능

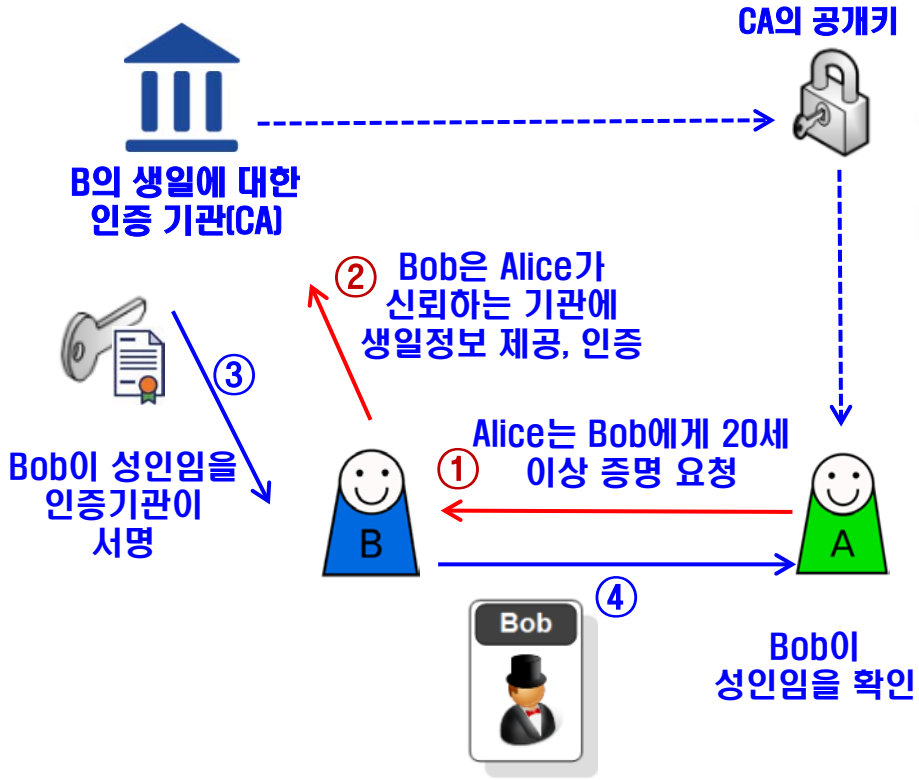
〈 secret sharing, multisignature, aggregated signature 기법 개념도 〉

공개키 기반 식별(Identification)과 정보 유출

- 기존 공개키 암호 기반 Identification 및 서명 사용 → 정보 유출
  - PKI 사용시, 발급자(issuer), subject 공개키, 인증 체인 정보 획득 가능
  - W3C에서 정의중인 DID(Decentralized Identifier)에서도 기존 PKI 사용시, 동일 문제 발생 → 프라이버시 보호를 위한 위임가능한 자격증명 (Delegatable Credential), 익명 인증(Anonymous Authentication) 등 사용 필요



〈 기존 PKI 사용시의 기업 프라이버시 침해 가능성〉

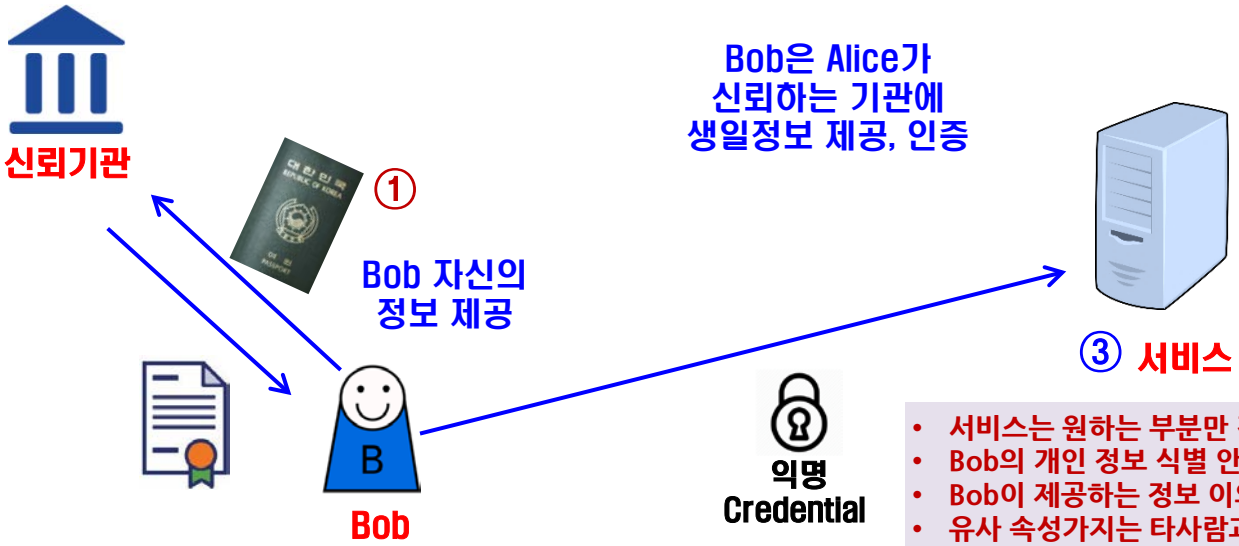


〈 Delegatable Credential 기반 Bob 프라이버시 보호〉

블록체인 암호 - 익명 Credential

익명 Credential 기법

- Credential(자격증명)
  - Identity 검증 혹은 인증 수단. 인증 정보 가짐. Certificate의 일부이거나 다른 인증 과정의 일부일 수 있음 (network 주소, security token 등)
- 익명 Credential
  - 기존 Certificate은 익명 Credential로 사용할 수 없음
  - 영지식 증명(interactive 혹은 Fiat-shamir), Commitment, Blind signature 사용 등



블록체인 암호 - 영지식 기반 프로토콜 사용

- 영지식 증명(zero-knowledge Proof) : 정보(ID 정보)를 노출하지 않으면서, 인증을 실현할 수 있음
- 예: Zerocash : Bitcoin상에서 프라이버시 보호를 위한 프로토콜, 영지식 증명
  - zk-SNARK 프로토콜 사용
  - Shamir Secret Sharing에서 사용한 Polynomial 기반 비밀정보 embedding 수행
  - 타원곡선 암호 기반 Hiding/Concealing 수행 (이산대수의 어려움)
  - 초기 trusted entit에 의한 초기 setup 과정 필요 (vs. Zerocoin : Trusted entity 필요 없음)
  - Zerocash 프로토콜 사용한 cryptocurrency : Zcash
- Zerocash 프로토콜 특성
  - 특성:
    - 288 byte proof per transactions (128-bit security)
    - <6 ms to verify a proof, <1 min to create
    - 896MB “system parameters”(fixed throughout system lifetime) → 40MB로 줄임
  - 사용하는 주요 암호 기법 : zk-SNARK
    - Homomorphic encryption을 위한 ECC 기반의 Pairing 사용
    - Knowledge of Exponent 기반 polynomial 위조 방지(Proof에 의한 위조)
    - SHA256, 서명, 영지식 증명 기법 사용 등

감사합니다

Q & A

부산대학교 전기컴퓨터공학부
부산대학교 사물인터넷 연구센터장
부산대 블록체인 플랫폼 연구센터장
부산대 융합보안대학원 책임교수

김호원
howonkim@pusan.ac.kr

참고 - 영지식 증명

영지식 증명(Zero-knowledge Proof)

– "증명 지식"을 밝히지 않고 주장의 정확성을 밝힘

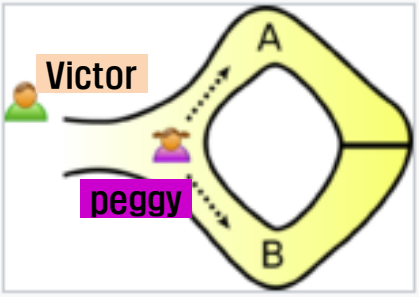
1. **peggy는** 동굴 안쪽 갈림길까지 들어와서, **두 개의 동굴 입구 중 어느 한쪽 방향을 임의로 선택한 후, 동굴 내부로 들어 감** (Victor는 동굴 밖에서 기다리고 있으므로 Peggy가 선택한 동굴 입구를 알지 못함)

2. 이후, **Victor는** 동굴 갈림길까지 와서 **동굴 입구 A/B 중에서 임의로 하나를 선택하여, Peggy에게 선택한 동굴 입구로 나오라(return)라고 함(Victor가 Peggy에게 입구 A로 나오라고 했다고 가정)**

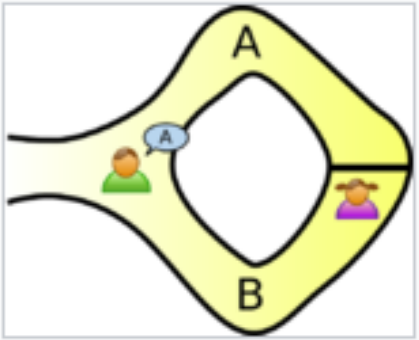
3. **Peggy가 중간문을 여는 "비밀번호"를 알고 있다면, Peggy는 쉽게 A로 올 수 있음** (이때, Peggy가 "비밀번호"를 모른다고 하더라도, 만약 peggy가 동굴 입구 A로 들어갔다면 A로 나올 수 있음)

4. **Victor가 위의 과정을 여러 번 반복하면서, random하게 A 혹은 B를 선택한다면, "Peggy가 비밀번호를 알 경우, Victory가 random하게 선택한 동굴 입구로 Peggy가 나올 수 있음"**

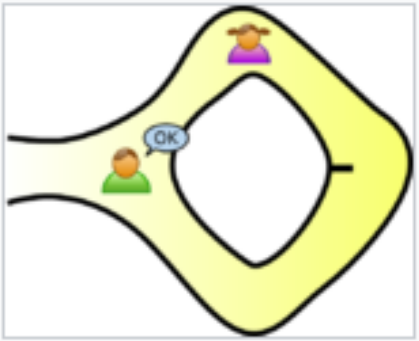
5. 이는 **Peggy는 자신이 알고 있는 비밀번호를 Victor한테 오픈하지 않고도 Peggy가 동굴 중간문의 비밀번호를 알고 있다는 주장이 증명됨 → 영지식 증명 !**



Peggy randomly takes either path A or B, while Victor waits outside



Victor chooses an exit path



Peggy reliably appears at the exit Victor names